Management Application Services

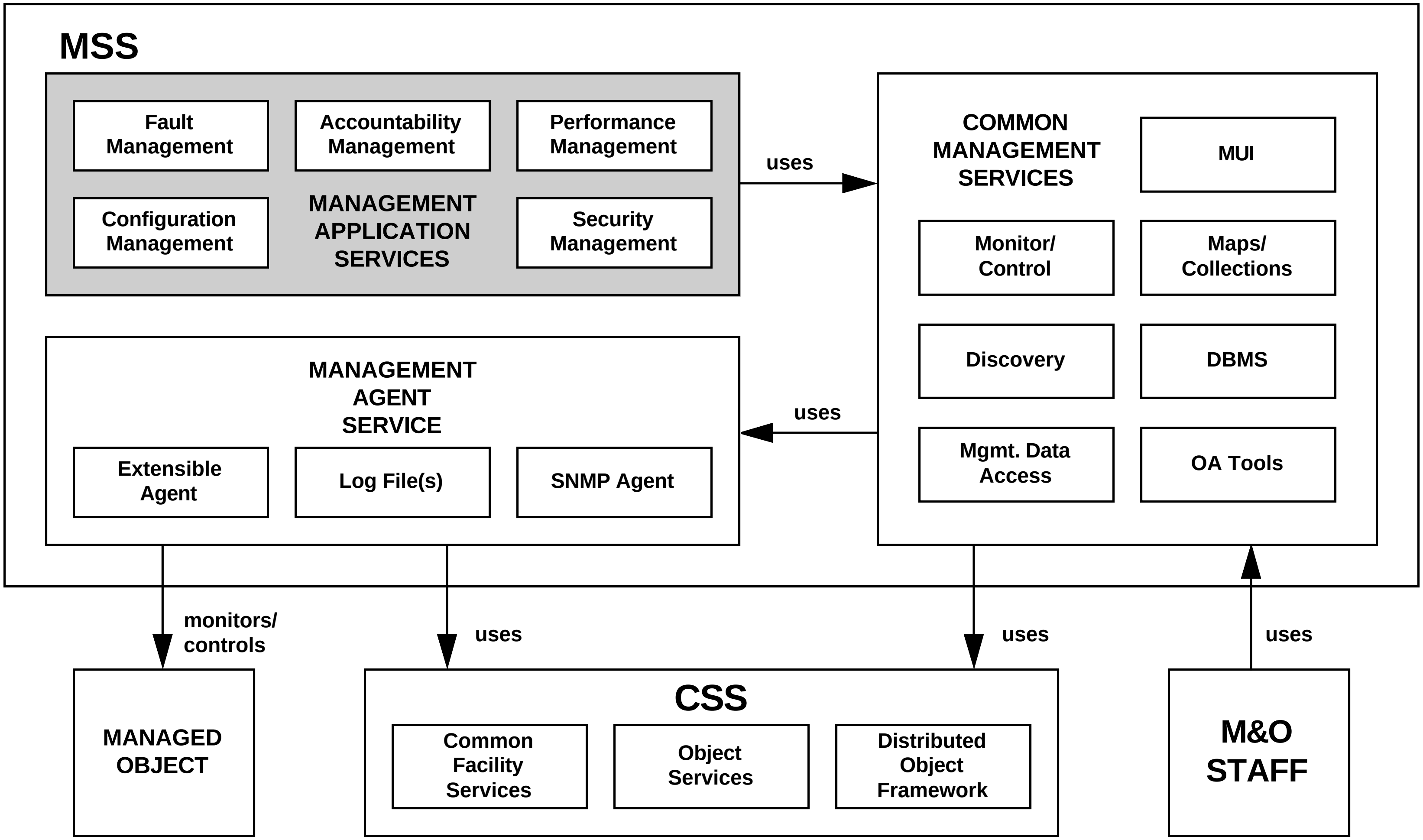
Yanamandra Sastry

19 January 1995

Management Application Services Roadmap

- **Performance Management**
- **Fault Management**
- **Security Management**
- **Accountability Management**

MSS Subsystem Design



MSS

Fault Management

Accountability Management

Performance Management

Configuration Management

MANAGEMENT APPLICATION SERVICES

Security Management

uses

COMMON MANAGEMENT SERVICES

MUI

Monitor/ Control

Maps/ Collections

Discovery

DBMS

Mgmt. Data Access

OA Tools

MANAGEMENT AGENT SERVICE

Extensible Agent

Log File(s)

SNMP Agent

uses

monitors/ controls

uses

uses

uses

MANAGED OBJECT

CSS

Common Facility Services

Object Services

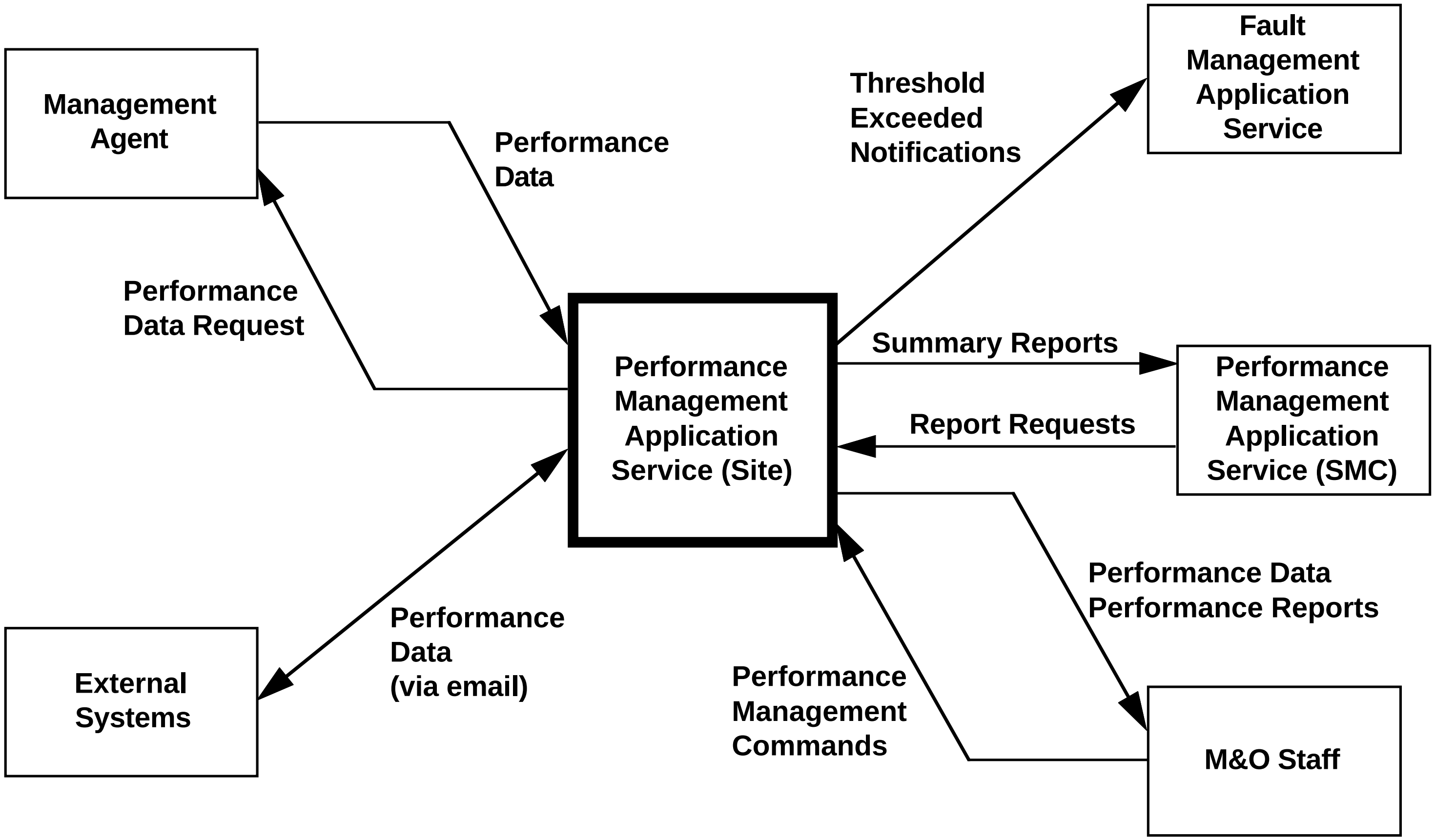
Distributed Object Framework

M&O STAFF

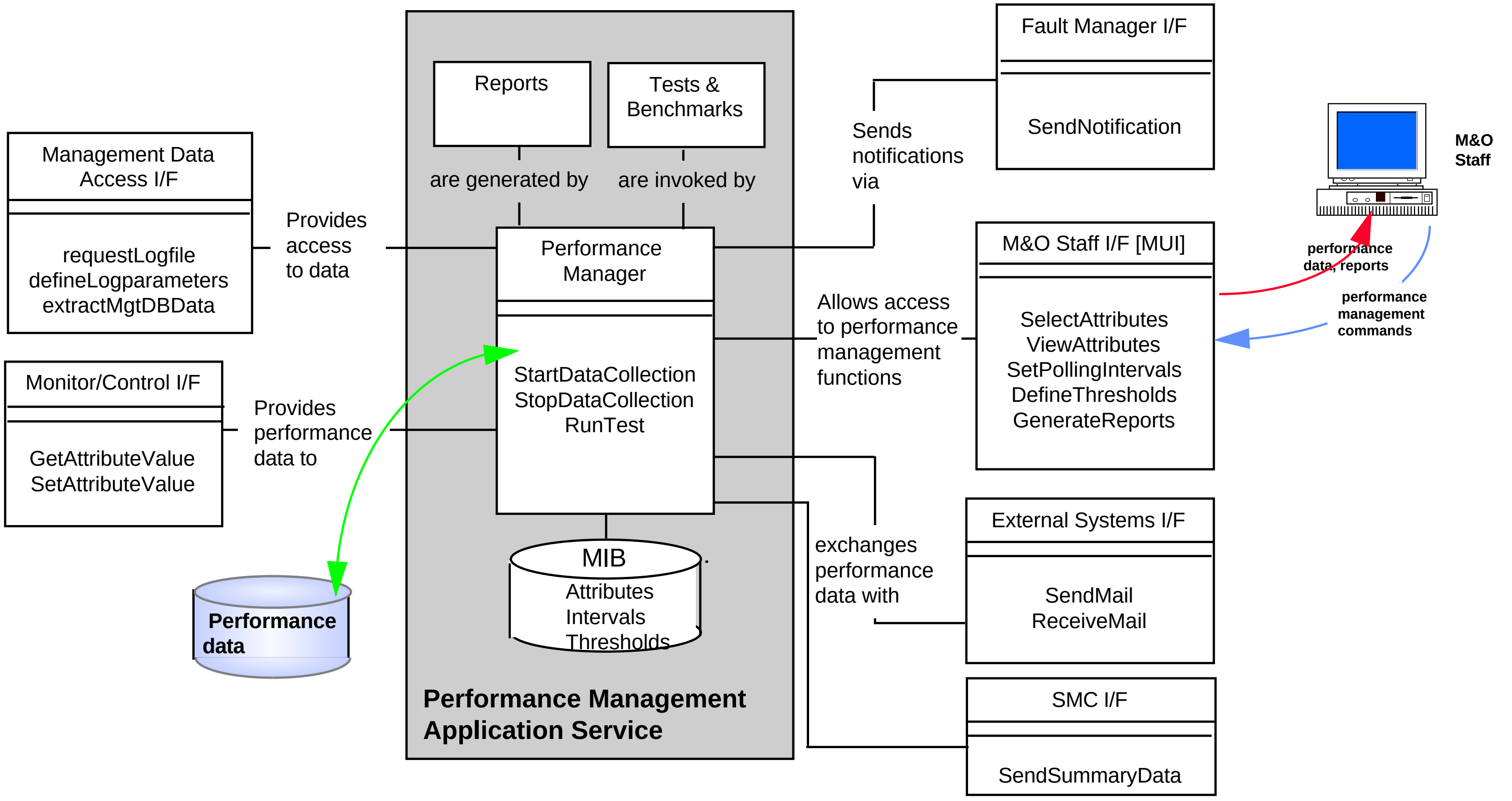
Performance Management Capabilities by Release

IR-1 capabilities	Release A capabilities
Monitoring and Analysis Network Monitoring Network Performance Monitoring Operating System Statistics Gathering **Reporting** Network Statistics Reporting Operating System Statistics Reporting	**Monitoring and Analysis** *Network Monitoring* *Network Performance Monitoring* *Operating System Statistics Gathering* Application Performance Data Collection Event Analysis **Testing** Network Tests & Benchmarks **Trending** Network Trends Analysis **Reporting** *Network Statistics Reporting* *Operating System Statistics Reporting* Application Performance Reporting

Performance Management Context


Management Agent
Performance Data
Performance Data Request
Threshold Exceeded Notifications
Fault Management Application Service
Performance Management Application Service (Site)
Summary Reports
Report Requests
Performance Management Application Service (SMC)
External Systems
Performance Data (via email)
Performance Data Performance Reports
Performance Management Commands
M&O Staff

Performance Management Design Decomposition



Management Data Access I/F

requestLogfile
defineLogparameters
extractMgtDBData

Provides access to data

Monitor/Control I/F

GetAttributeValue
SetAttributeValue

Provides performance data to

Performance data

Reports

are generated by

Tests & Benchmarks

are invoked by

Performance Manager

StartDataCollection
StopDataCollection
RunTest

MIB

Attributes
Intervals
Thresholds

Performance Management Application Service

Sends notifications via

Fault Manager I/F

SendNotification

Allows access to performance management functions

M&O Staff I/F [MUI]

SelectAttributes
ViewAttributes
SetPollingIntervals
DefineThresholds
GenerateReports

M&O Staff

performance data, reports

performance management commands

exchanges performance data with

External Systems I/F

SendMail
ReceiveMail

SMC I/F

SendSummaryData

Performance Management Scenario

Performance degradation alert from a host:

1. Performance Manager is used, via M&O Staff I/F, to select the attribute of CPU utilization on the LSM server, to set a data collection interval of 5 seconds and to establish a threshold of 70% on the metric
2. Performance Manager is used to establish an alert notification upon the threshold being exceeded
3. Performance Manager receives the value of this attribute every interval via the Monitor/Control I/F
4. Performance Manager compares the returned value against the established threshold
5. In one interval, the CPU utilization of the LSM server exceeds the threshold
6. Performance Manager detects that the threshold is crossed, generates a notification via the Fault Manager I/F
7. M&O Staff, via the M&O Staff I/F, generate and view a CPU utilization graph for the LSM server

Performance Management Scenario (cont.)

8. Performance Manager instantiates the requested report from the stored performance data
9. The report shows CPU utilization at 65% all day, with a narrow peak above 70% utilization
10. M&O Staff, via the M&O Staff I/F, generate another CPU utilization report for the previous five days. The report indicates a steady increase from 55% to 70%
11. Further, another report is generated to review CPU utilization by process. This report indicates that the CPU utilization of security server on the LSM server has increased steadily over the 5 days to 95% of the total CPU utilization
12. The Accountability Management Service (covered later in the presentation) is then used to review Accountability data for activities of the security server. This analysis shows a dramatic increase in authentication and authorization records indicating an increase in the use of the security server
13. This directly corresponds to a new service that was made available the previous week

Solution: The security server is replicated across a second LSM workstation for the purpose of balancing the load on the first server. This results in the lowering of CPU utilization on the original LSM server

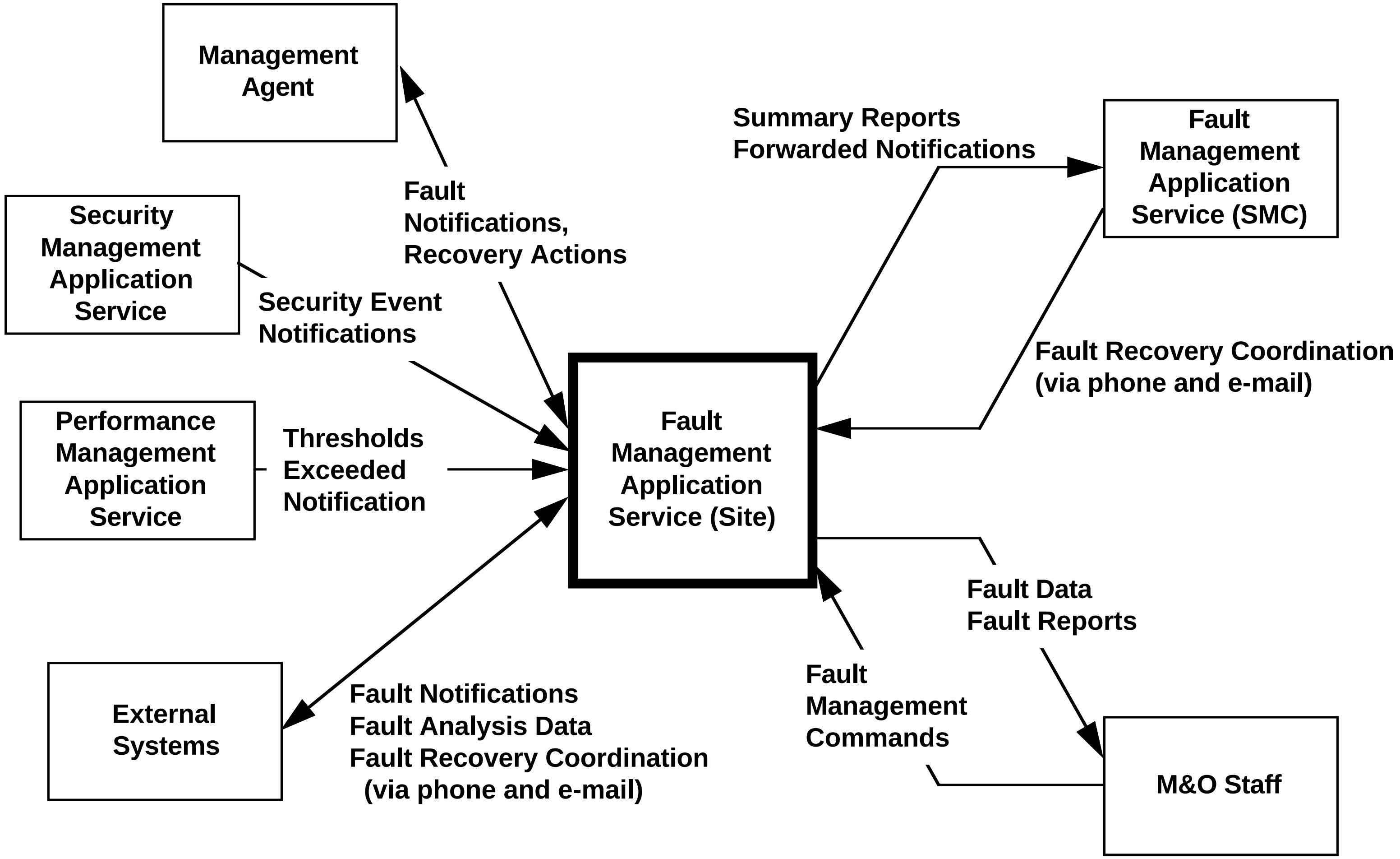
Management Application Services Roadmap

- Performance Management
- **Fault Management**
- Security Management
- Accountability Management

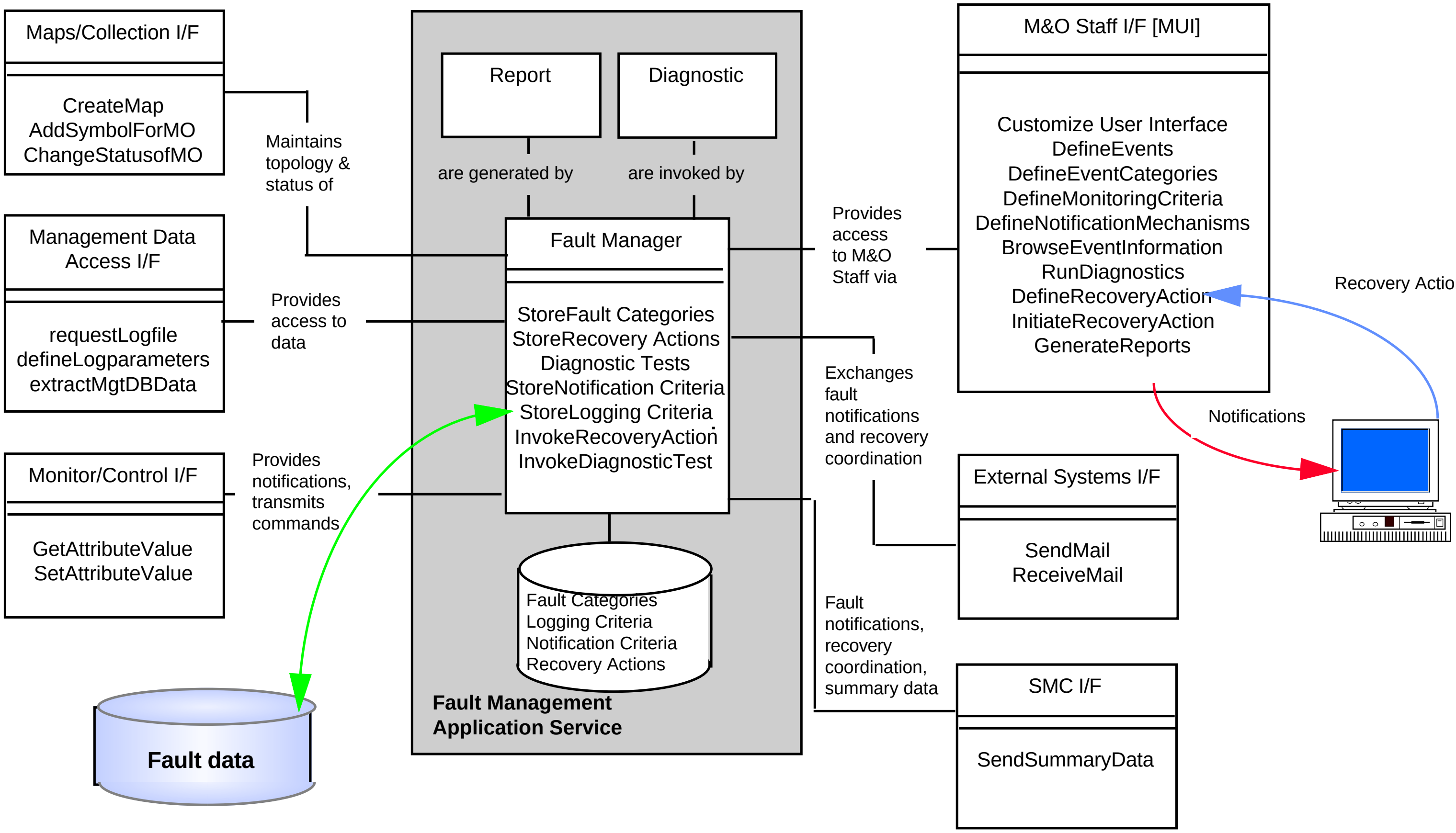
Fault Management Capabilities by Release

IR-1 capabilities	Release A capabilities
Detection Faults associated with: Routers Communication Lines Hosts (Also available in Release A)	**Detection** Faults associated with: Operating Systems Peripheral Devices Application Processes Exceeding of Performance Thresholds
Notification Network Event Logging Visual & Audible Notifications	**Notification** *Network Event Logging* *Visual & Audible Notifications* Event logging for hosts, operating systems, peripherals and applications Event Log Analysis Alarm Processing
Isolation & Diagnosis Vendor Diagnostics of COTS hardware Event Log Browser	**Isolation & Diagnosis** *Vendor Diagnostics of COTS hardware* *Event Log Browser*

Fault Management Context


Management Agent
Fault Notifications, Recovery Actions
Summary Reports Forwarded Notifications
Fault Management Application Service (SMC)
Security Management Application Service
Security Event Notifications
Fault Recovery Coordination (via phone and e-mail)
Performance Management Application Service
Thresholds Exceeded Notification
Fault Management Application Service (Site)
Fault Data Fault Reports
External Systems
Fault Notifications Fault Analysis Data Fault Recovery Coordination (via phone and e-mail)
Fault Management Commands
M&O Staff

Fault Management Design Decomposition



Maps/Collection I/F

CreateMap
AddSymbolForMO
ChangeStatusofMO

Maintains topology & status of

Management Data Access I/F

requestLogfile
defineLogparameters
extractMgtDBData

Provides access to data

Monitor/Control I/F

GetAttributeValue
SetAttributeValue

Provides notifications, transmits commands

Fault data

Report

are generated by

Diagnostic

are invoked by

Fault Manager

StoreFault Categories
StoreRecovery Actions
Diagnostic Tests
StoreNotification Criteria
StoreLogging Criteria
InvokeRecoveryAction
InvokeDiagnosticTest

Fault Categories
Logging Criteria
Notification Criteria
Recovery Actions

Fault Management Application Service

Provides access to M&O Staff via

M&O Staff I/F [MUI]

Customize User Interface
DefineEvents
DefineEventCategories
DefineMonitoringCriteria
DefineNotificationMechanisms
BrowseEventInformation
RunDiagnostics
DefineRecoveryAction
InitiateRecoveryAction
GenerateReports

Recovery Actions

Notifications

Exchanges fault notifications and recovery coordination

External Systems I/F

SendMail
ReceiveMail

Fault notifications, recovery coordination, summary data

SMC I/F

SendSummaryData

Fault Management Scenario

Host Failure

1. Fault Manager receives notification of host failure from management agent via Monitor/Control I/F
2. Fault Manager generates visual (changes color of icon and/or a pop-up window) and audible notifications according to specified criteria
3. The M&O Staff I/F is used to browse the event log for diagnostic information
4. M&O Staff I/F is then used to traverse the map hierarchy to determine whether other hosts on the LAN are reachable
5. Fault Manager is used to initiate a test to determine the reachability of the problem host from the LSM server. The test fails
6. Fault Manager is used to initiate a test to determine the reachability of the problem host from another host. This test fails too
7. Fault Manager is used to determine the status of the interfaces of the host. The test indicates that they are down
8. This confirms that the host is down, which is then rebooted

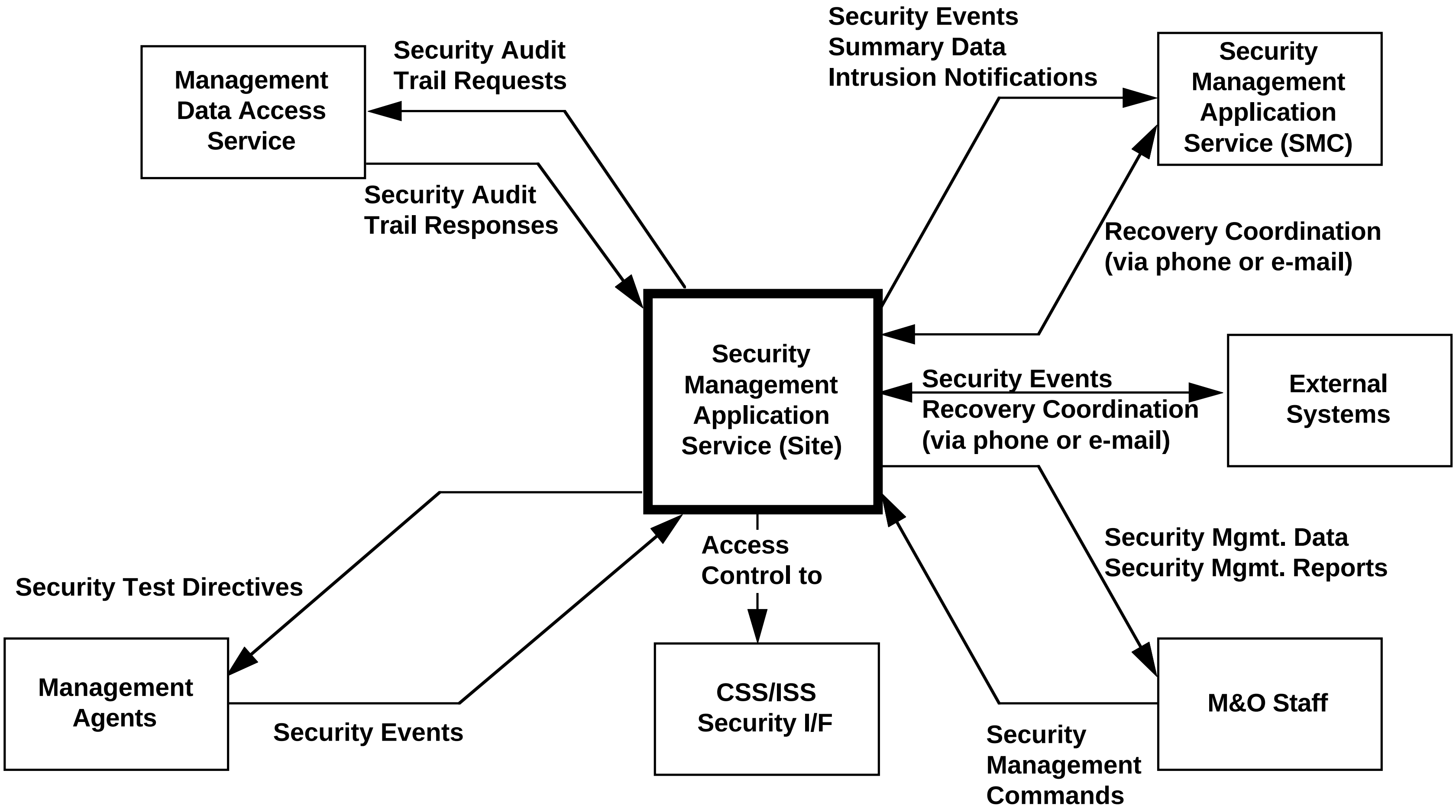
Management Application Services Roadmap

- Performance Management
- Fault Management
- **Security Management**
- Accountability Management

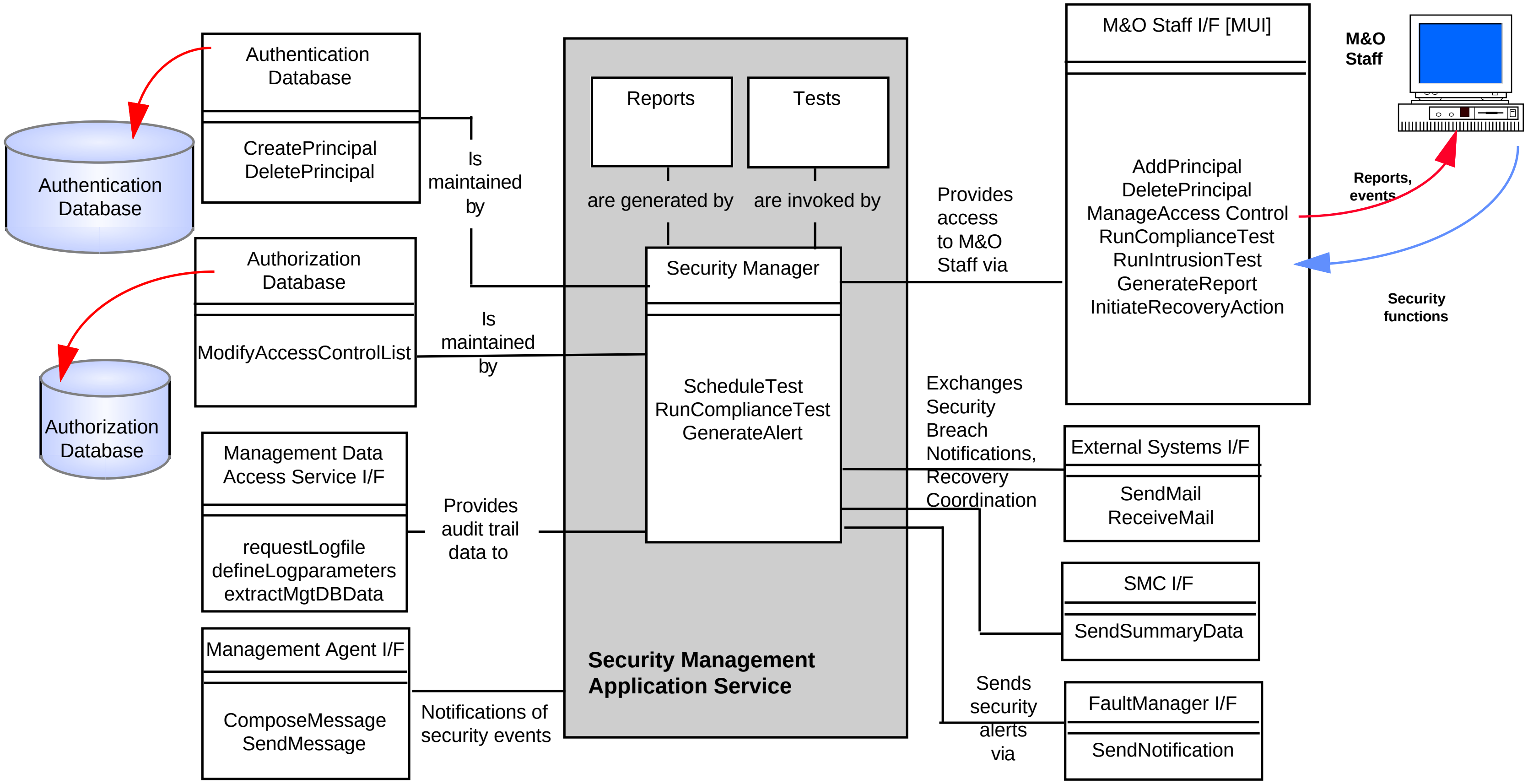
Security Management Capabilities by Release

IR-1 capabilities	Release A capabilities
Security Database Management	**Security Database Management**
Router-based Address Filtering	*Router-based Address Filtering*
Network-Based Authentication	*Network-based Authentication*
Host-Based Authorization	*Host-based Authorization*
	Network-based Authorization
User Registration	**Compliance Management**
Account Management	Password Auditing
	Privilege Auditing
	File System Integrity Checking
	Intrusion Detection
	Virus Checking
	Unauthorized User Access Detection
	Reporting
	Security Audit Trail Reports
	Compliance Management Reports
	Intrusion Detection Reports

Security Management Context



Security Management Design Decomposition



Authentication Database

Authentication Database

CreatePrincipal
DeletePrincipal

Is maintained by

Authorization Database

Authorization Database

ModifyAccessControlList

Is maintained by

Management Data Access Service I/F

requestLogfile
defineLogparameters
extractMgtDBData

Provides audit trail data to

Management Agent I/F

ComposeMessage
SendMessage

Notifications of security events

Reports

Tests

are generated by

are invoked by

Security Manager

ScheduleTest
RunComplianceTest
GenerateAlert

Security Management Application Service

Provides access to M&O Staff via

M&O Staff I/F [MUI]

AddPrincipal
DeletePrincipal
ManageAccess Control
RunComplianceTest
RunIntrusionTest
GenerateReport
InitiateRecoveryAction

M&O Staff

Reports, events

Security functions

Exchanges Security Breach Notifications, Recovery Coordination

External Systems I/F

SendMail
ReceiveMail

SMC I/F

SendSummaryData

Sends security alerts via

FaultManager I/F

SendNotification

Security Management Scenario

Intrusion Detection:

1. ECS Security policy requires that Compliance Tests be run periodically
2. Security Manager allows the periodicity of running the test to be configurable
3. A DAAC with no history of breakins decides to schedule these tests weekly. The Security Manager is set up accordingly, accessed via the M&O Staff I/F, to schedule weekly execution of the test
4. As a result of a scheduled test, the Security Manager receives a notification, via the Management Agent I/F that a .rhosts file (a security hole) has been discovered in the home directory of an account
5. Security Manager sends a notification of the event via the Fault Manager I/F according to specified criteria maintained by the Security Manager
6. M&O Staff, via the M&O Staff I/F, discover that the date of creation of the file is the current date

(The owner of the account has been on vacation for three days, which indicates that the account has been compromised)

Security Management Scenario (cont.)

7. Upon initiation by the M&O Staff, via the M&O Staff I/F, security audit data is accessed by Security Manager via Data Management Access I/F to view data records for the activity on the compromised account
8. The activity on the account has been only the previous day, with several login failures spaced far apart in time so as not to trip the login failure alert. This indicates that the password has been guessed
9. A check of users currently logged on reveals that the compromised account is not currently in use, and the compromised account is disabled
10. The M&O Staff notifies the other DAACs, via the External Systems I/F about the incident

Solution:

The host is taken off-line for further investigation and analysis. Local site policy is modified to run Compliance Tests on a daily basis.

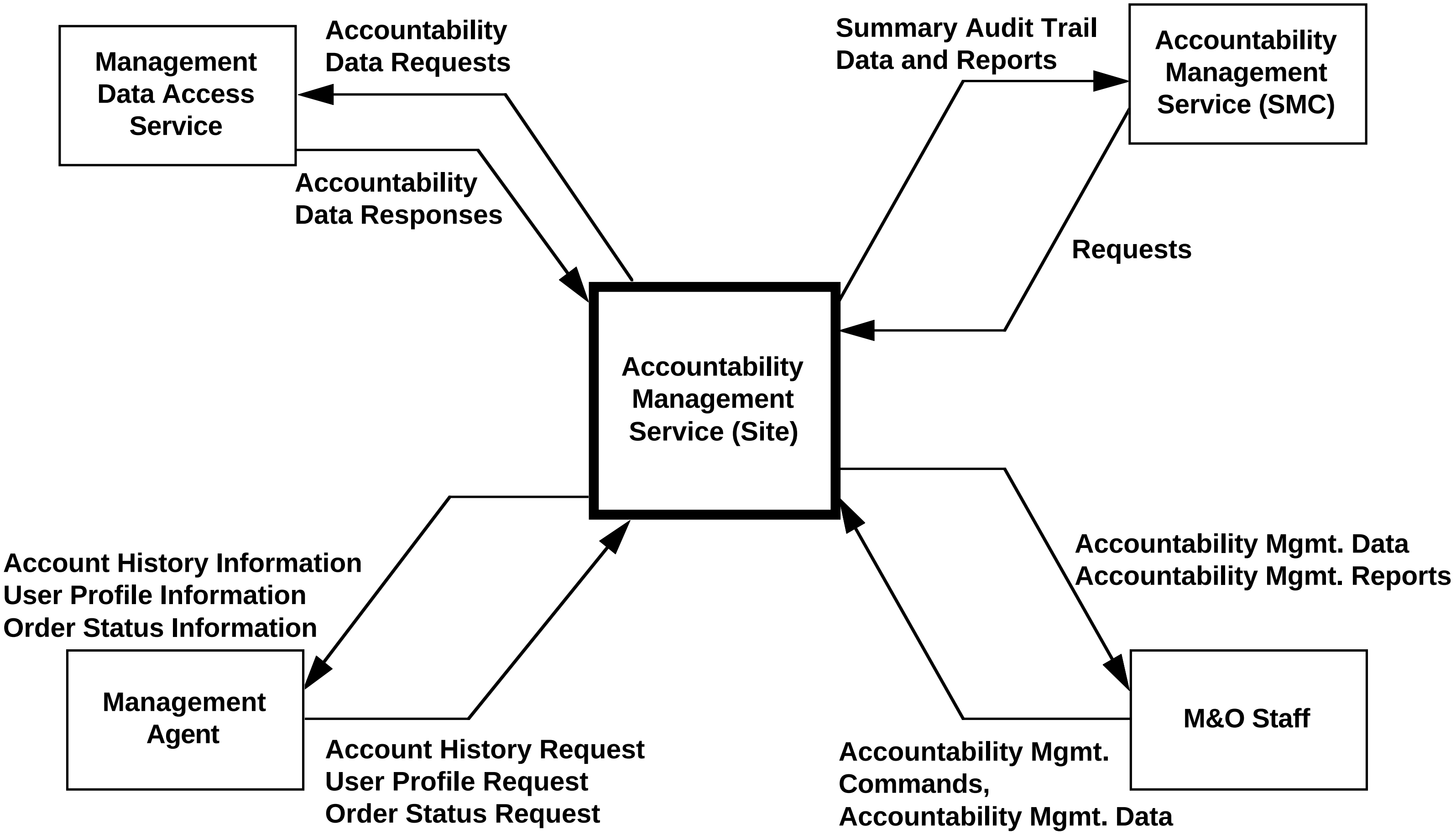
Management Application Services Roadmap

- Performance Management
- Fault Management
- Security Management
- **Accountability Management**

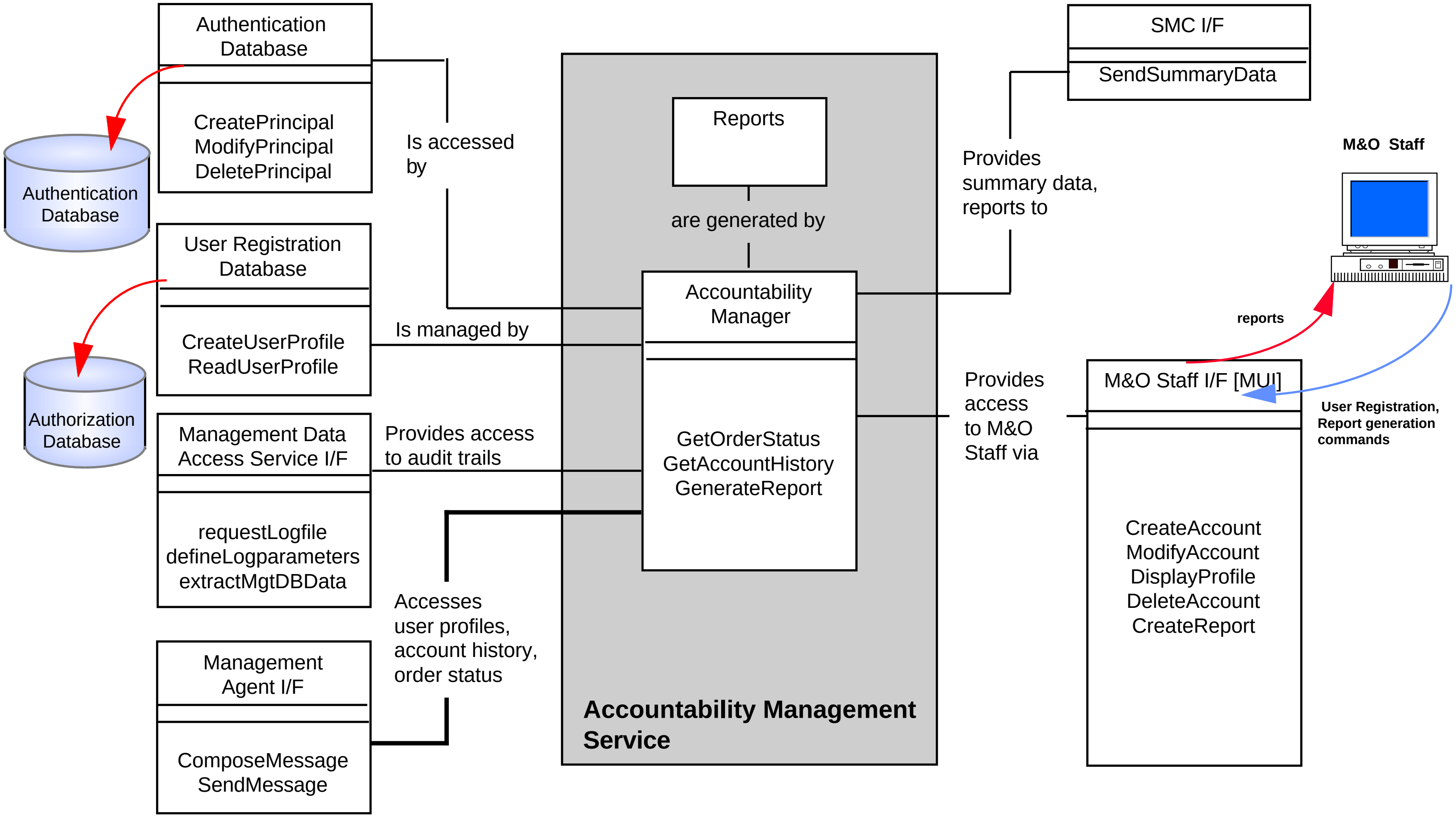
Accountability Management Capabilities by Release

IR-1 capabilities	
No implementation in IR-1	**User Registration** AccountCreation **User Audit Trail** Account History Status User Accountability Trail **Data Audit Trail** Order Status **Report Generation**

Accountability Management Context


Management Data Access Service
Accountability Data Requests
Accountability Data Responses
Summary Audit Trail Data and Reports
Accountability Management Service (SMC)
Requests
Accountability Management Service (Site)
Account History Information
User Profile Information
Order Status Information
Management Agent
Account History Request
User Profile Request
Order Status Request
Accountability Mgmt. Data
Accountability Mgmt. Reports
M&O Staff
Accountability Mgmt. Commands,
Accountability Mgmt. Data

Accountability Management Design Decomposition



Accountability Management Scenario

Pre-Condition:

1. ESDIS distributes a list of pre-approved users to the DAACs
2. A user accesses ECS as a guest user (needs no password)
3. The guest user wishes to become a registered user
4. The guest user fills out electronic (or manual) application form
5. The application form is sent to the appropriate DAAC
6. The M&O Staff responsible for user registration processes the application
7. The M&O Staff forwards the application for approval to the DAAC management and the established point of contact for the affiliated project

User Registration - New users

1. The M&O Staff accesses Accountability Manager via the M&O Staff I/F for User Registration
2. Accountability Manager provides access to create an entry in the Authentication Database, and to create a corresponding entry in the User Registration Database
3. The new user receives notification of the new account with the password and access procedures via US mail

Management Application Services Summary

Service	Key Technology Selection	Migration and Evolution
Performance Management	- SNMP V1 - Standards based (DME 2.0) - HP-OpenView selected	SNMP V2, CORBA, CMIP
Fault Management	- SNMP V1 - Standards based (DME 2.0)	SNMP V2, CORBA, CMIP, Event correlation
Security Management	- DCE	SNMP V2
Accountability	- DCE RPCs, RDBMS, SQL	CORBA